PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/14, 12/54, H04Q 7/38 — A1

(11) International Publication Number: WO 97/33403

(43) International Publication Date: 12 September 1997 (12.09.97)

(21) International Application Number: PCT/FI97/00139

(22) International Filing Date: 3 March 1997 (03.03.97)

(30) Priority Data:
960996 4 March 1996 (04.03.96) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Upseerinkatu 1, FIN-02600 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: KARI, Hannu [FI/FI]; Kullervonkuja 9 B 9, FIN-02880 Veikkola (FI). KARPPANEN, Arto [FI/FI]; Vattuniemenkatu 4 D 64, FIN-00210 Helsinki (FI).

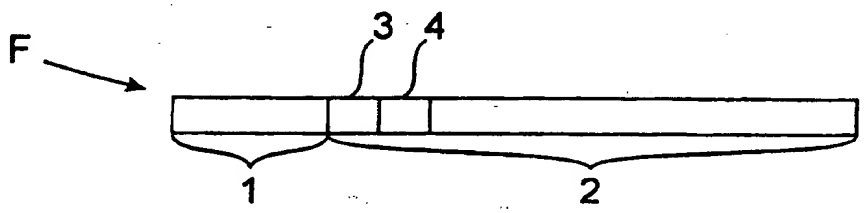
(74) Agent: KOLSTER OY AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: IMPROVING SECURITY OF PACKET-MODE TRANSMISSION IN A MOBILE COMMUNICATION SYSTEM

(57) Abstract



In General Packet Radio Service GPRS, the data are coded into frames (F) with a given length and comprising a header (1) and a data portion (2). An intruder can interfere with GPRS communication by transmitting unauthorized copies of transmitted messages, or sending false messages and interfere with communication integrity. The reliability of GPRS communication is improved by modifying the frame (F) used on a GPRS connection so that possible extra copies of the frames can be revealed. This can be achieved e.g. by adding an extra information field (3) to the data portion (2) of a GPRS frame (F), the contents of the field being modified between two frames (F). The contents of the extra information field (3) can include the identity of the frame (F), the TLLI of the connection, the IMSI or MSISDN of the mobile station, or an identity formed by an algorithm generating pseudo-random numbers. A second extra information field (4) can be added to the data portion (2) of the frame (F), the field being preferably formed by a different algorithm than the first extra information field (3).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

IMPROVING SECURITY OF PACKET-MODE TRANSMISSION IN A MOBILE COMMUNICATION SYSTEM

The invention relates to improving the security of packet-mode data transmission in a mobile communication system.

Figure 1 shows the parts of a cellular mobile communication system essential to the invention. Mobile Stations MS communicate with Base Transceiver Stations BTS over the air interface Um. The base stations are controlled by Base Station Controllers BSC associated with Mobile Switching Centres MSC. A subsystem administered by a base station controller BSC - including the base stations BTS controlled by it - is commonly called a Base Station Subsystem BSS. The interface between a centre MSC and a base station subsystem BSS is called the A-interface. The section of the A-interface on the side of the mobile services switching centre MSC is called a Network Subsystem NSS. Correspondingly, the interface between a base station controller BSC and a base station BTS is called the Abis-interface. A mobile services switching centre MSC switches incoming and outgoing calls. It performs similar tasks as the centre of a public telephone network PSTN. Additionally, it performs tasks characteristic of mobile telecommunication only, such as subscriber location administration, in co-operation with network subscriber registers (not separately shown in Figure 1).

A typical radio connection used in digital mobile communication systems is circuit switched, i.e. the radio resources reserved for a subscriber are kept reserved for that connection during the whole call. General Packet Radio Service GPRS is a new service designed for digital mobile communication systems, such as the GSM system. The packet radio service has been described in the ETSI recommendation TC-TR-GSM 01.60. A packet-mode radio connection with effective utilization of radio resources can be offered to a user of a mobile station MS by means of the packet radio service. In a packet switched connection resources are reserved only when there is speech or data to be transmitted. The speech or data is assembled into packets with a given length. Such a packet having been transmitted over the air interface Um, and the transmitting party having no immediately succeeding packets to be transmitted, the radio resource can be released to the use of other subscribers.

In order to illustrate the description, but not to limit the invention, it is assumed that the system comprises a separate GPRS service control node, or a GPRS Support Node GSN, which controls the operation of the packet

data service on the network side. This control comprises e.g. mobile station Logon and Logoff, mobile station location updates, and routing of data packets to the right destination. As regards the present application, the term "data", widely interpreted, refers to any information exchanged in a digital mobile communication system, such as speech coded in digital form, data transmission between computers, or telefax data. A GSN node can be situated in connection with a base station BTS, a base station controller BSC or a mobile services switching centre MSC, or apart from these. The interface between a GSN node and a base station controller BSC is called the Gb-interface.

Referring to Figure 1 and 2, information, such as control signalling and user data, is exchanged between a mobile station and a GSN node by means of GPRS frames. Each Frame F comprises at least a header 1 and a data portion 2. In order for the system to know which mobile station has transmitted the frame, the header 1 comprises an identifier for the mobile station, e.g. a Temporary Logical Link Identity TLLI. At the beginning of a connection, the GSN node assigns to a mobile station a TLLI to be used during a GPRS connection. After the GPRS connection, the same TLLI can be reassigned to another mobile station.

In addition to a TLLI, a Network Layer Service access point Identity NLSI can also be used in the header 1 to indicate the application protocol used by the mobile station.

The data portion 2 comprises confidential information, e.g. user data or control messages. This kind of information has to be protected in order to prevent data transfer to third parties in a comprehensible form. The data portion 2 can be coded, i.e. encrypted by an encryption key, known only to the transmitter and the receiver of the message. Since mobile stations use divided resources instead of connection-specific radio resources, the header 1 cannot be similarly protected. If the headers were protected by encryption, each receiver would have to open the headers of all messages transmitted over the air interface Um. Only then could a mobile station MS know to which mobile station the message was intended, or a GSN node could know which mobile station MS transmitted the message. The GSN node does not necessarily know which encryption key to use.

As the header of a frame cannot be protected, the above prior art packet-mode data transmission involves certain security problems. Hence a third party, such as an intruder or an eavesdropper can interfere with GPRS

communication over the air interface Um. In the present application such a person or device is referred to as an intruder. This term covers all kinds of unauthorized interference with communication over the air interface irrespective of whether the purpose of the interference is eavesdropping, disturbing communications, or any other unexceptional operation, e.g. an attempt to garble charging data. Even if the intruder is unable to unravel the contents of the message, (s)he may cause disturbance by using a TLLI intercepted from the air interface. The intruder may e.g. interfere with GPRS communication by transmitting unauthorized copies of messages transmitted via a GPRS connection, or send false messages and interfere with communication integrity. A typical control message is quite short and even if the intruder does not know the encryption key, (s)he may try to find it out by a large-scale attack.

It is an object of the invention to provide a method for preventing the above possibility to interfere with GPRS communication and for improving communication reliability. The objects of the invention are achieved with a method which is characterized by what is disclosed in the characterizing part of claim 1. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on improving the reliability of GPRS communication by modifying a frame used on a GPRS connection so that frames sent by an intruder can be identified. This can be achieved e.g. by adding an extra information field to the data portion of a GPRS frame, the contents of the field being known only to the transmitter and the receiver of the message. In the present application the term "an extra information field" refers to a field added to the data portion of a frame not in order to transmit data but to improve communication reliability. The simplest way to implement this is to have the mobile communication system and a mobile station negotiate an encryption algorithm and/or the parameters used by such an algorithm when the mobile station registers for use of a data transmission service. Negotiation can take place even at the beginning of a data connection and possibly even during a new connection. This kind of protection prevents an intruder from transmitting false messages at least for a while as (s)he does not know which encryption algorithm and/or parameter is being used. If the contents of the extra field do not comply with the protocol negotiated between the transmitter and the receiver, the frame may be rejected.

An intruder can, however, send copies of frames (s)he has inter-

cepted and interfere with communication integrity. Such interference can be prevented by modifying the contents of the extra information field between two successive frames sent over the air interface. In a simple and computationally preferable manner the extra information field is formed different in each successive frame, e.g. so that the contents of each extra field comprise the GPRS frame number. The receiver can compare the frame number in the extra field with the frame number normally used on the connection, the number being sent either in the frame header, or alternatively the transmitter and the receiver can generate it themselves by assigning running numbers to the frames. If the frame number in the extra field does not comply with the frame number normally used on the connection, the frame may be rejected.

In accordance with a preferable embodiment of the invention the protection is further improved. Although an intruder does not know the encryption key, (s)he may try to guess its contents and send random messages. At worst a receiver can interpret such a message as a command, e.g. a Logoff message causing connection setdown. By sending numerous random messages an intruder may interfere with communication on a GPRS connection, and hence is it preferable to further improve the protection. This can be done e.g. by adding another extra information field to the data portion of a GPRS frame, the contents of the field being formed by a different algorithm and/or parameters than the contents of the first extra information field.

An advantage of the protection conforming with the invention is that an intruder cannot send unauthorized copies of messages transmitted on a GPRS connection. This is because the intruder does not know the algorithm and/or the parameters used in forming the extra information field. By placing an extra information field in the data portion of a frame, instead of the header, the mechanism for protecting the data portion by encryption, implemented in several systems, can be utilized. The protection of the invention is simple to implement. The data transmission layer and the layer handling encryption are independent of the method of the invention. Modifications may be needed in the message handling operations above or parallel to the encryption layer only. The operation of network elements between the transmitter and the receiver does not have to be modified. For these network elements the extra field of the invention is completely transparent. It has the same appearance as the rest of the contents of the data portion of a GPRS frame.

The invention is described further hereinafter, in connection with

preferable embodiments, with reference to the accompanying drawings, in which:

Figure 1 shows the parts of a mobile telephone network essential to the invention;

Figure 2 shows the structure of a conventional GPRS frame used in communication between a mobile station and a GSN node;

Figure 3 shows the structure of a secured GPRS frame of the invention; and

Figure 4 shows the structure of a double-secured GPRS frame of the invention.

Figure 3 shows the structure of a secured GPRS frame F of the invention. Let us assume first that the invention is applied to a system where the data portion of frame F is transmitted encrypted so that the encryption key is modified between two successive frames. Compared with a conventional frame shown in Figure 2, an extra information field 3 is added to the data portion 2 of frame F of the invention, the contents of the field being different in each successive frame. The contents of the extra information field 3 can be simply the number of frame F. The receiver, i.e. a GSN node or a mobile station MS, can compare the frame number in the extra field 3 with the frame number normally used on the connection and sent in the frame header 1. Alternatively the transmitter and the receiver can develop the frame number themselves by assigning running numbers to frames F. If the frame number in the extra field 3 does not comply with the frame number normally used on the connection, the receiver may reject the frame.

It is essential to the protection of the invention that the contents of the extra information field 3 are different in two successive frames sent over the air interface. In this case the contents of the extra information field 3 can also be the same in two successive frames before encryption as the extra information fields 3 in successive frames are made different by encryption. The contents of the extra information field 3 before encryption can be e.g. one of the following either wholly or partially:

- a constant
- the IMSI or MSISDN identity of a mobile station;
- a connection-specific identity; or
- a pseudo-random number.

The identity of a mobile station can be its IMSI or MSISDN identity.

In some systems, a difference may be made between the identity of a terminal and the identity of a mobile subscriber. As regards the invention, it is irrelevant whether the used identity identifies a terminal or a subscriber. As regards the invention, the identity of a mobile station may also be temporary, e.g. an identity negotiated between the transmitter and the receiver.

A connection-specific identity is an identity independent of the identity of a mobile station or a subscriber. It may be the identity TLLI of a temporary logical connection used on the connection. It may also be an identity a mobile station and a GSN node negotiate when the mobile station registers for use of a data transmission service. A mobile station and a GSN node may also negotiate a new temporary identity at the beginning of each connection or during the connection.

A pseudo-random number is a number developed by a suitable pseudo-random algorithm so that only the transmitter and the receiver are aware of the used algorithm and/or the used parameters. Even if the algorithm generating the random number is in general knowledge, it may be thought that several alternative algorithms are in use, and the transmitter and the receiver negotiate the algorithm to be used one at a time. A random number has to be interpreted widely so that the term covers any form of a bit sequence. It is hence not necessary to confine oneself to bit groups corresponding to e.g. BCD coded numbers.

If the invention is applied to a system where the data portion 2 of frame F is not sent encrypted, the contents of the extra information field 3 can be formed by an algorithm generating pseudo-random numbers so that the contents of field 3 are modified as soon as possible between two frames F sent over the air interface Um. For security, it is preferable to use an algorithm that modifies the contents of field 3 between each two frames F.

Figure 4 shows the structure of a GPRS frame conforming with a preferred embodiment of the invention. To further improve security, the data portion 2 of frame F also contains another information field 4. The contents of the other extra information field 4 can be formed by one of the above algorithms, the algorithm being preferably different from the one used to form the first extra information field 3. Alternatively the same algorithm can be used to form the extra information fields 3 and 4, but with different parameters. If the data portion 2 of frame F is not sent encrypted, e.g. frame F number and an algorithm generating pseudo-random numbers can be used to form the infor-

mation fields 3 and 4.

It is not absolutely necessary for the contents of the extra information fields 3 and/or 4 to be different in all frames used during the connection. The algorithm generating pseudo-random numbers, or at least one of them, may also be cyclic.

It is obvious to those skilled in the art that the basic inventive idea can be implemented in a variety of ways. In the description of the invention it has been assumed, for the sake of clarity, that the functions controlling the packet radio operation have been concentrated to a GSN node. These functions can, however, be integrated with other network elements, such as a base station, a base station controller, or a mobile services switching centre. In this case the sections of the network elements concerned controlling packet radio operation have to be understood to replace the GSN node. The other extra information field used in a preferred embodiment of the invention is an illustrative concept, too. One may also think that one extra information field consists of two or more portions generated by two or more different algorithms, respectively. Thus, the invention and its embodiments are not restricted to the above examples, but may vary within the scope of the claims.

CLAIMS

1. A method for data transmission between a transmitter and a receiver (MS, GSN) in a digital mobile communication system comprising at least one mobile station (MS) and at least one air interface (Um), in which method:

- the data to be transmitted is assembled into frames (F) comprising at least a header (1) and a data portion (2); and

- frames (F) are transmitted only when there is need for data transmission;

characterized in that:

- an extra information field (3) is added to the data portion (2) of a frame (F), and

- the transmitter and the receiver (MS, GSN) negotiate between themselves an algorithm and/or a parameter on the basis of which the contents of the extra information field (3) are formed.

2. A method as claimed in claim 1, **characterized** in that the algorithm and/or parameter are negotiated when a mobile station (MS) registers for use of a data transmission service.

3. A method as claimed in claim 1, **characterized** in that the algorithm and/or parameter are negotiated at the beginning of each connection.

4. A method as claimed in claim 3, **characterized** in that the algorithm and/or parameter are renegotiated during the connection.

5. A method as claimed in claim 1, **characterized** in that the contents of the extra information field (3) are modified between two successive frames (F) transmitted over the air interface (Um).

6. A method as claimed in any one of claims 1 to 5, **characterized** in that the data portions (2) of the frames (F) are transmitted encrypted over the air interface (Um) and the extra information field (3) comprises at least one of the following identities:

- a bit sequence constant
- the identity of the frame (F) concerned or a portion thereof;
- the IMSI or MSISDN identity of the mobile station;
- a connection-specific identity; or
- a pseudo-random number.

7. A method as claimed in any one of claims 1 to 5, **charac-**

terized in that the extra information field (3) comprises an identity formed by an algorithm generating pseudo-random numbers, whereby the data portions (2) of the frames (F) can be sent encrypted or unencrypted over the air interface (Um).

8. A method as claimed in any one of claims 1 to 7, characterized in that to improve protection, at least one second extra information field (4) is added to the data portion (2) of a frame (F), the field comprising at least one of the following identities:

- a bit sequence constant
- the identity of the frame (F) concerned or a portion thereof;
- the IMSI or MSISDN identity of the mobile station;
- a connection-specific identity; or
- a pseudo-random number.

9. A method as claimed in claim 8, characterized in that at least one of the second extra information fields (4) comprises a different identity than the first extra information field (3).

Fig. 1

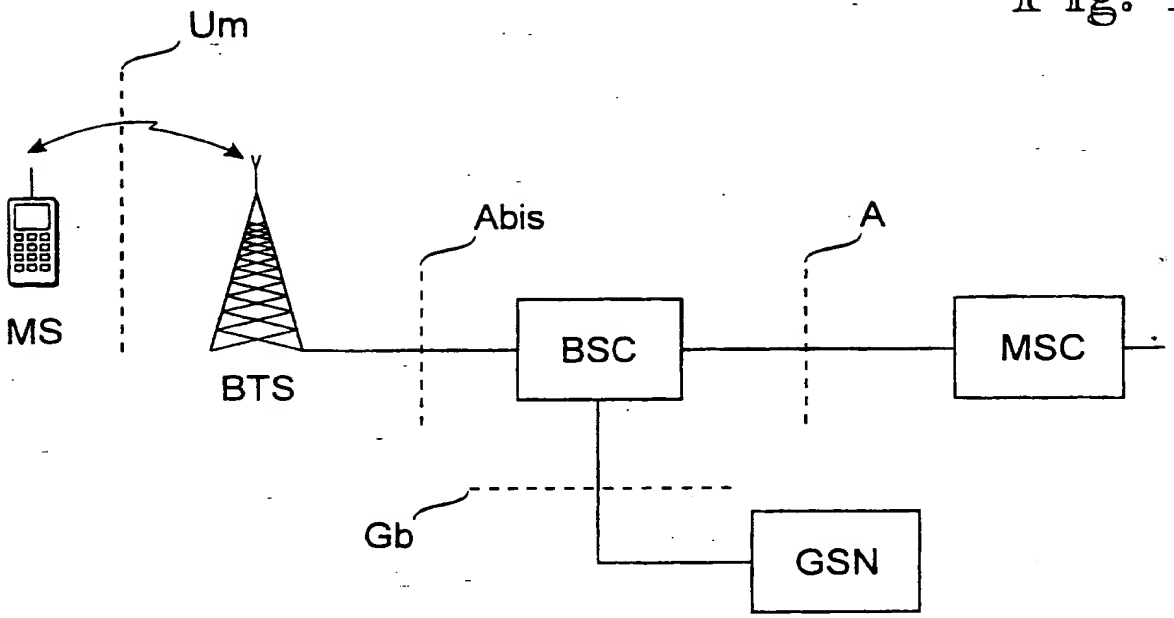


Fig. 2

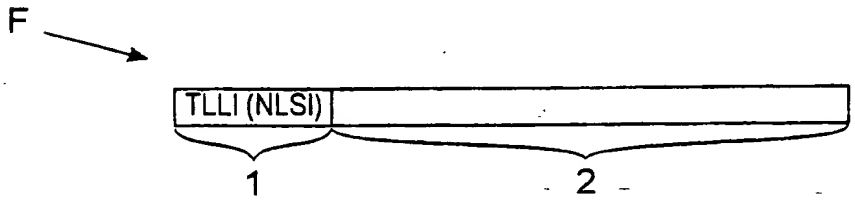


Fig. 3

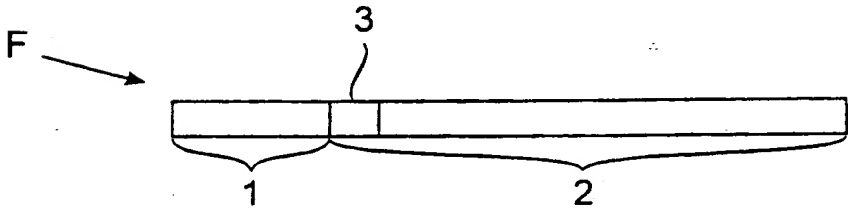
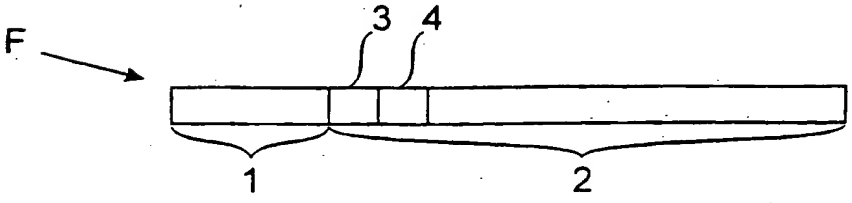


Fig. 4



INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00139

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/14, H04L 12/54, H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0689316 A2 (AT & T CORP.), 27 December 1995 (27.12.95), column 2, line 58 - column 3, line 13; column 3, line 42 - column 4, line 44, abstract --	1-9
A	US 5455863 A (DANIEL P. BROWN ET AL), 3 October 1995 (03.10.95), column 3, line 37 - line 51; column 4, line 37 - line 56; column 7, line 63 - column 8, line 47 -- --------	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 June 1997	19 -06- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Kenneth Ahrengart Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT
Information on [redacted] family members

03/06/97

International application No.
[redacted] FI 97/00139

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0689316 A2	27/12/95	CA 2149067 A	23/12/95
		JP 8032575 A	02/02/96
US 5455863 A	03/10/95	CA 2141318 A	12/01/95
		EP 0663124 A	19/07/95
		FI 950714 A	17/02/95
		JP 8500950 T	30/01/96
		WO 9501684 A	12/01/95